Hong Kong University of Science and Technology

COMP170: Discrete Mathematical Tools for Computer Science

Spring 2009

Midterm Exam 2

21 April 2009, 3:00–4:20pm, LT-E

Solutions

Question 1: From the encryption step of the RSA algorithm, we know that

$$C = M^e \bmod n,$$

where $(e, n) = (173, 481)$ is the public key of Bob.

We also know that n is the product of two prime numbers p and q, i.e., $n = pq$. Let $T = (p-1)(q-1)$.

From the decryption step of the RSA algorithm, we can recover M as

$$M = C^d \bmod n,$$

where d is the multiplicative inverse of e in Z_T, i.e., $de \bmod T = 1$.

One way to break the RSA encryption is to factorize n. Since $n = 481 = 13 \cdot 37$, we let $p = 13$ and $q = 37$. Hence, $T = 12 \cdot 36 = 432$.

The multiplicative inverse d satisfies the following equation:

$$de = kT + 1 \quad \text{or} \quad 173d = 432k + 1$$

for some integer k. We note that $d = 5$ satisfies the equation for $k = 2$.

The original plaintext M can be found as follows:

$$\begin{aligned} M &= 22^5 \bmod 481 \\ &= ((22^2 \bmod 481)^2 \cdot 22) \bmod 481 \\ &= (3^2 \cdot 22) \bmod 481 \\ &= 198. \end{aligned}$$

Question 2: Alice computes

$$A = m^a \bmod n$$

and sends it to Bob.

Similarly, Bob computes

$$B = m^b \bmod n$$

and sends it to Alice.

Upon receiving A from Alice, Bob computes

$$K_1 = A^b \bmod n = m^{ab} \bmod n.$$

Similarly, upon receiving B from Bob, Alice computes

$$K_2 = B^a \bmod n = m^{ab} \bmod n.$$

Since $K_1 = K_2 = m^{ab} \bmod n$, it is the key shared by Alice and Bob.

This scheme (and the key) is secure because

$$f(a) = m^a \bmod n$$
$$g(b) = m^b \bmod n$$

are one-way functions, in the sense that it is easy to compute $f(a)$ and $g(b)$ from a and b but it is difficult to compute a and b from $f(a)$ and $g(b)$.

Question 3: (a) False.

The remainder is equal to $7^{1980} \bmod 47$. Since 47 is prime and $\gcd(7, 47) = 1$, we can apply a variant of Fermat's little theorem to compute the remainder as

$$7^{1980 \bmod 46} \bmod 47 = 7^2 \bmod 47 = 2 \neq 1.$$

(b) False.

If $p = \mathrm{F}, q = \mathrm{T}, r = \mathrm{F}$, then the truth value of the first statement is T but that of the second statement is F.

(c) False.

It suffices to prove that the negation of the statement, i.e.

$$\neg\exists x \in Z^+ \, (\forall y \in Z \, (x + y \geq 4))$$

or

$$\forall x \in Z^+ \, (\exists y \in Z \, (x + y < 4))$$

is true.

For every $x \in Z^+$, we can choose $y = 4 - x - 1 \in Z$ to satisfy the inequality $x + y < 4$. So we are done.

(d) True.

We can prove this by induction.

For the base case ($x = 1$), 6 divides $x^3 - x = 1 - 1 = 0$ because any positive integer divides 0. So the base case holds.

For $x > 1$, we assume that it holds for $x - 1$, i.e., $6 \mid ((x-1)^3 - (x-1))$. To show that $6 \mid (x^3 - x)$, it suffices to show that $6 \mid ((x^3 - x) - ((x-1)^3 - (x-1)))$. Because $(x^3 - x) - ((x-1)^3 - (x-1)) = 3x^2 - 3x = 3x(x-1)$ and $x(x-1)$ is an even number (i.e., 2 is a divisor) for all $x > 1$, so both 2 and 3 divide $3x(x-1)$ and hence 6 also divides it.

By the principle of MI, we can prove the correctness of the statement.

(e) False.

One counterexample is the prime number $p = 5$, but $p! + 1 = 121 = 11^2$ is composite.

Question 4: (a) (i) $\forall x \, (\mathrm{Student}(x) \Rightarrow \mathrm{Smart}(x))$

(ii) $\exists x \, (\mathrm{Politician}(x) \wedge \neg\mathrm{Smart}(x))$

(b) Statement (i) in part (a) can be expressed equivalently by its contrapositive as follows:

$$\forall x \, (\neg\mathrm{Smart}(x) \Rightarrow \neg\mathrm{Student}(x))$$

By combining this with statement (ii) using a form of modus ponens, we obtain

$$\exists x \, (\mathrm{Politician}(x) \wedge \neg\mathrm{Student}(x))$$

which means 'some politicians are not university students'.

Question 5: We prove the correctness of the following statement for all $n \geq 1$ by induction:

> $S(n)$: The smallest number of disk moves required to solve the Towers of Hanoi puzzle with n disks is $2^n - 1$.

- **Base case:** $(n = 1)$
  For $n = 1$ disk, $2^1 - 1 = 1$. Obviously this is the smallest number of moves required. So $S(1)$ holds.
- **Inductive step:** $(n > 1)$
  We assume that $S(n-1)$ holds as the inductive hypothesis, i.e., the smallest number of moves required for $n-1$ disks is $2^{n-1} - 1$.
  We now consider the puzzle with n disks. At some point the top $n-1$ disks on the leftmost peg must be stacked on a separate peg so that the bottom disk can be moved to the rightmost peg. By the inductive hypothesis, this takes a minimum of $2^{n-1} - 1$ moves, and moving the bottom disk adds at least one more move. When the bottom disk settles on the rightmost peg and won't move anymore, we need to bring the smaller $n-1$ disks on top of it. Notice that, while the bottom disk makes this final move from the leftmost peg to the rightmost peg, all other $n-1$ disks must be stacked on the middle peg. Again by the inductive hypothesis, in order to bring all $n-1$ smaller disks from the middle peg to the rightmost peg, we need at least $2^{n-1} - 1$ moves. Adding up, the smallest number of moves required for n disks is $(2^{n-1} - 1) + 1 + (2^{n-1} - 1) = 2^n - 1$ and hence $S(n)$ holds.

By the principle of mathematical induction, we can conclude that $S(n)$ holds for all $n \geq 1$.

Question 6: We prove the statement for the existence of a binary representation for every positive integer by strong induction.

- **Base case:** $(n = 1)$
  Clearly this case just corresponds to $a_0 = 1$.
- **Inductive step:** $(n > 1)$
  We assume that it holds for all positive integers $< n$ and prove that it also holds for n.
  If n is even, then $n/2$ is a positive integer less than n. So, by the inductive hypothesis, it can be expressed as
  $$\frac{n}{2} = a_r 2^r + a_{r-1} 2^{r-1} + \cdots + a_2 2^2 + a_1 2 + a_0.$$
  Therefore,
  $$n = a_r 2^{r+1} + a_{r-1} 2^r + \cdots + a_2 2^3 + a_1 2^2 + a_0 2 + 0.$$
  If n is odd, then $(n-1)/2$ is a positive integer less than n and can be expressed as
  $$\frac{n-1}{2} = a_r 2^r + a_{r-1} 2^{r-1} + \cdots + a_2 2^2 + a_1 2 + a_0.$$
  So we have
  $$n = a_r 2^{r+1} + a_{r-1} 2^r + \cdots + a_2 2^3 + a_1 2^2 + a_0 2 + 1.$$
  For both cases we prove that the statement also holds for n.

By the principle of mathematical induction, we can conclude that the statement holds for all positive integers n.

Question 7: We first iterate the recurrence for $S(n)$:

$$\begin{aligned} S(n) &= 3S(n-1) + 4 \\ &= 3(3S(n-2) + 4) + 4 \\ &= 3^2 S(n-2) + 4(3+1) \\ &= 3^3 S(n-3) + 4(3^2 + 3 + 1) \\ &\ \ \vdots \\ &= 3^n S(0) + 4\sum_{i=0}^{n-1} 3^i \\ &= 3^n + 4\frac{3^n - 1}{3-1} \\ &= 3^n + 2\cdot 3^n - 2 \\ &= 3^{n+1} - 2. \end{aligned}$$

So $S(n-1) = 3^n - 2$. Substituting it into the recurrence relation for $T(n)$ gives

$$T(n) = \begin{cases} 1 & n = 0 \\ 2T(n-1) + g(n) & n > 0 \end{cases}$$

where $g(n) = 3^{n+1} - 6$.

We now iterate this recurrence for $T(n)$ as follows:

$$\begin{aligned} T(n) &= 2T(n-1) + g(n) \\ &= 2(2T(n-2) + g(n-1)) + g(n) \\ &= 2^2 T(n-2) + 2g(n-1) + g(n) \\ &= 2^3 T(n-3) + 2^2 g(n-2) + 2g(n-1) + g(n) \\ &\ \ \vdots \\ &= 2^n T(0) + \sum_{i=0}^{n-1} 2^i g(n-i) \\ &= 2^n + \sum_{i=0}^{n-1} 2^i (3^{n-i+1} - 6) \\ &= 2^n + 3^{n+1} \sum_{i=0}^{n-1} \left(\frac{2}{3}\right)^i - 6\sum_{i=0}^{n-1} 2^i \\ &= 2^n + 3^{n+1}\frac{1-(2/3)^n}{1-2/3} - 6\frac{2^n - 1}{2-1} \\ &= 2^n + 3^{n+2} - 9\cdot 2^n - 6\cdot 2^n + 6 \\ &= 3^{n+2} - 14\cdot 2^n + 6. \end{aligned}$$

Since

$$\Theta(S(n)) = \Theta(3^{n+1} - 2) = \Theta(3\cdot 3^n) = \Theta(3^n)$$

and

$$\Theta(T(n)) = \Theta(3^{n+2} - 14\cdot 2^n + 6) = \Theta(9\cdot 3^n) = \Theta(3^n),$$

so $\Theta(S(n)) = \Theta(T(n))$.